

**Electronic payment gateway system of security transaction and independent authority****Publication number:** TW388021B**Publication date:** 2000-04-21**Inventor:** HUANG JR-MING (TW); CHEN MAU-TAI (TW); LIAN JIAN-CHIN (TW); YANG TZ-WEN (TW); LI JIAN-HUEI (TW)**Applicant:** CHUNGWHA TELECOM LAB (TW)**Classification:****- international:** G07F1/00; H04L9/00; G07F1/00; H04L9/00; (PC1-7); G06F17/60; G07F1/00; H04L9/00**- European:****Application number:** TW19990113992 19990817**Priority number(s):** TW19990113992 19990817[Report a data error here](#)**Abstract of TW388021B**

An electronic payment gateway system of security transaction and independent authority is a new design for electronic transaction which utilizes one-way hashed password principle in combination with CA public/private key to develop a system that the entire secure transaction flow process is controlled by the security control center and the approval center verifies if the personal identification and message are correct to ensure the identification confirmation message integrity, non-duplicated order, high fault tolerance and transparent transaction flow process. In addition, this system does not have additional economical overhead and import/export restriction in terms of technology, so it can be globally adapted by numerous financial facilities and is more acceptable than the current security system of electronic commerce, in particular when the material flow center is taken into account. It is the system that has the purchase flow designs for both verification and registration.

Data supplied from the **esp@cenet** database - Worldwide

LEARNING TECH

www.learningtech.com.tw

中華民國專利資訊網

seednet

see your needs

專利分類專區


專利分類專區 | 註冊專利號碼查詢專區 | 審查專區 | 最

快速檢索 | 布林檢索 | 關位檢索 | 進階檢索 | 案件狀態檢索

\*\*本系統專利資料僅供參考, 不作爲准駁依據, 所有資料以經濟部智慧財產局公告爲準 | 中文造字安裝程式: (約1.6M)

## 00388021 -- 核准公告專利公報資料

## 安全交易及授權獨立之電子付款控管系統

專利公告號	00388021 說明書影像 / 圖式影像 / 權利異動 / 雜項資料 / 
卷號	27
期號	12
公告日期	2000/04/21
專利類型	發明
國際專利分類號	G06F 17/60, G07F 1/00, H04L 9/00
申請案號	0088113992
申請日期	1999/08/17
申請人	中華電信股份有限公司電信研究所; 桃園縣楊梅鎮民族路五段五五一巷十二號
發明人	黃志明 陳茂太 連建欽 楊子文 李建輝 黃志雄 張光耀
代理人資訊	江舟峰; 台北市長安東路二段八十一號六樓
摘要	<p>一種安全交易及授權獨立之電子付款控管系統, 係爲</p> <p>一電子交易付款新設計, 利用單向雜湊密碼(One-way Hashed Password)原理, 配合CA公私鑰之運用, 發展一套由</p> <p>安控中心主控整個安全交易流程並由認證中心驗證身份及</p> <p>訊息之正確, 達到身份確認、訊息完整性、訂單不被複</p> <p>製、高容錯力及交易流程透明等目的; 且沒有經濟上額外</p> <p>的負擔, 技術也沒有進出口限制, 並可擴大至世界上無數</p> <p>的金融單位; 比現在電子商務使用的安全系統更容易接</p> <p>受, 尤其是物流中心也納入考慮, 是一兼具認證及存證之</p> <p>購物流程設計。</p>
<input type="checkbox"/> 申請專利範圍	<p>1. 一種安全交易及授權獨立之電子付款控管系統, 包括有: 第一循環: 確認消費者及交易識別序號, 利用單向雜湊密碼做身份確認, 密碼由本系統之安控中心, 統一</p>

存的資料是單向雜湊值, 所以安控中心可以在不知道密碼值的情況下進行身份確認中心;

不可否認之簽名模組, 電子交易付款時, 安控中心通常需要檢查使用者付款帳單上之雜湊密碼原理的加解密就可確認是否為使用者真實的簽名;

第二階段: 購買商品的處理, 包括訂貨、送貨、取貨、扣款等之資料傳送;

所有傳送之資料均經特殊處理, 不僅保證資料不被竊取, 且確認各項資料的所有者身份與訂單的唯一性。

2. 如申請專利範圍第 1 項所述之安全交易及授權獨立之電子付款控管系統, 其中該安儲存於資料庫的單向雜湊密碼來確認使用者的身份, 確認身份的步驟如下:

步驟一: 安控中心送出測試值  $anc$  給使用者, 以確認其身份,  $n$  是安控中心產生的亂數

步驟二: 係用者以其密碼  $Pc$ , 計算

$(anc) Pc$  並回傳給安控中心;

步驟三: 因為  $(anc) Pc = (acPc) n$ , 所以安控中心根據資料庫儲存的單向雜湊密碼  $acPc$  使用者之身份。

圖式簡單說明:

第一圖為本創作之安全交易及授權獨立之電子付款控管系統架構圖;

第二圖為一般網際網路安全交易環境; 以及

第三圖為安全交易及授權獨立之電子付款控管系統之電子交易架構圖。

達華科技股份有限公司 (c) Copyright 2003 Learningtech Corp. TEL: +886-3-402-4200 · 402-4201 Fax: +886-3-402-4632